IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

MICHAEL O'BRADOVICH, individually and on behalf of all others similarly situated, Plaintiff, v. CHANGE HEALTHCARE INC.; OPTUM, INC.; and UNITEDHEALTH GROUP INC., Defendants.	Case No. 2:24-cv-00452 **COMPLAINT—CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Michael O'Bradovich ("Plaintiff") brings this Class Action Complaint on behalf of himself and all others similarly situated, against Defendants Change Healthcare, Inc. ("Change"), Optum, Inc. ("Optum"), and UnitedHealth Group Inc. ("UnitedHealth"), (collectively "Defendants"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to himself, which are based on personal knowledge.

NATURE OF THE ACTION

1. "Desperate patients around the country have been forced to choose between paying out of pocket for essential medications or forgoing them entirely as the aftermath of a cyberattack on a major health care company stretches into its third week."[1] This is the reality that patients across the country face in light of data breach that the Department of Health and Human Services

[1] https://www.nbcnews.com/health/health-care/cyberattack-change-healthcare-patients-struggle-get-medication-rcna141841 (last visited March 25, 2024).

has called "the most significant and consequential incident of its kind against the U.S. health care system in history."[2]

2. Change, a subsidiary of UnitedHealth's Optum division, offers healthcare technology services including, *inter alia*, revenue cycle management, healthcare analytics, and payment processing for patients, healthcare providers, and pharmacies. Change is one of the world's largest processors of health and medical data and patient records, handling upwards of 15 billion healthcare transactions annually.[3] Change is critical to the nation's healthcare system, helping facilitate healthcare transactions between healthcare providers and most major insurance companies.

3. On February 21, 2024, UnitedHealth discovered threat actors had breached part of Change's information technology network, forcing Defendants to take Change's systems offline (the "Data Breach").[4] The threat actors responsible for the Data Breach claim to have stolen six terabytes of information during the Data Breach, including the personally identifying information ("PII") and protected health information ("PHI") of millions of individuals, including but not limited to: medical records, insurance records, dental records, payment information, claims information, health data, contract information, and Social Security Numbers.[5]

---

[2] Rick Pollack, *AHA Statement on HHS Response to Change Healthcare Cyberattack*, American Hospital Association (Mar. 5, 2024), https://www.aha.org/press-releases/2024-03-05-aha-statement-hhs-response-change-healthcare-cyberattack.

[3] Zack Whittaker, *As the Change Healthcare Outage Drags On, Fears Grow That Patient Data Could Spill Online*, TechCrunch (Mar. 9, 2024), https://techcrunch.com/2024/03/09/change-healthcare-fears-data-breach-ransomware/; Change Healthcare, https://www.changehealthcare.com/ (last visited Mar. 25, 2024).

[4] https://www.healthcaredive.com/news/change-cyberattack-unitedhealth-nation-state/708328/ (last visited Mar. 25, 2024).

[5] Steve Alder, *UHG Identifies Attack Vector Used in Change Healthcare Ransomware Attack*, HIPAA Journal (Mar. 15, 2024), https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/#:~:text=The%20group%20claims%20to%20have,information%2C%20and%20Social%20Security%20numbers.

4. The fallout from the Data Breach has been widespread and severe causing disruptions to the healthcare system across the United States. The Data Breach has left healthcare providers "unable to check patients' eligibility for treatment or fill prescriptions electronically."[6] This has had devastating impact on patients, with reports of patients "being billed hundreds or more than a thousand dollars for prescriptions that previously were covered by insurance;" some not being able to fill their prescriptions filled at all; and still others not being able to apply discount coupons to afford their medications.[7]

5. The Data Breach and the disruption to patients' access to their needed medications was foreseeable and the direct and proximate result of Defendants' failure to implement adequate data security measures to protect its systems from unauthorized access.

6. As healthcare business associates under federal law, Defendants knowingly obtain, collect, and store patient PII and PHI—and have a duty to secure, maintain, protect, and safeguard the PII and PHI in their possession against unauthorized access and disclosure through reasonable and adequate data security measures. Defendants are also well-aware that the PII and PHI is highly valuable to cybercriminals, making it highly foreseeable that Defendants would be the target of a cyberattack.

---

[6] *Outages from Change Healthcare cyberattack causing financial 'mess' for doctors*, NBC News (March 1, 2024), https://www.nbcnews.com/news/us-news/outages-change-healthcare-cyberattack-causing-financial-mess-doctors-rcna141321

[7] Marlene Cimons et al., *How a health-care cyberattack may affect your prescription drug access,* Washington Post (March 5, 2024), https://www.washingtonpost.com/wellness/2024/03/05/change-healthcare-hack-prescriptions-affect/

7. Despite these duties and the foreseeability of a data breach, however, Defendants failed to implement adequate data security measures, leading to a data breach of "unprecedented magnitude" and the disruption of patients' access to their medications.[8]

8. In order to recover to Defendants' wrongful conduct, Plaintiff on behalf of himself and a similarly situated class of individuals, brings claims for negligence, negligence *per se*, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

PARTIES

9. Plaintiff Michael O'Bradovich is an adult who is a resident and citizen of the Commonwealth of Pennsylvania. Although Defendants failed to notify him that his data was implicated in the Data Breach, Plaintiff discovered the Data Breach and has since learned that his PII and/or PHI in Change's possession has likely been compromised in the Data Breach.

10. Defendant Change Healthcare, Inc. ("Change") is a Delaware corporation with a principal place of business located in Nashville, Tennessee. Change was acquired by UnitedHealth Group Inc. in 2022 and now operates as a unit of Optum, Inc., providing data analytics and medical transaction services.

11. Defendant Optum, Inc. ("Optum") is a Delaware corporation with a principal place of business located in Eden Prairie, Minnesota. Optum is a subsidiary of UnitedHealth Group Inc., focused on data analytics, pharmacy care, and healthcare delivery and operations.

12. Defendant UnitedHealth Group Inc. ("UnitedHealth") is a Delaware corporation with a principal place of business located in Minnetonka, Minnesota. UnitedHealth provides health

[8] *HHS Office for Civil Rights Issues letter and Opens Investigation of Change Healthcare Cyberattack*, U.S.' Dep't of Health & Human Servs. (Mar. 13, 2024), https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html.

insurance and healthcare services globally, and is the world's largest healthcare company by revenue.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendants.

14. This Court has general jurisdiction over Optum pursuant to Pa. C.S.A. § 5301. Specifically, this Court has general jurisdiction over Optum because Optum is an out-of-state corporation registered to do business under the laws of the Commonwealth of Pennsylvania since May 9, 2000. As part of registering to do business in the Commonwealth of Pennsylvania, Optum "shall enjoy the same rights and privileges as a domestic entity and shall be subject to the same liabilities, restrictions, duties and penalties . . . imposed on domestic entities." Pa. C.S.A. § 402(d). Among other things, Pennsylvania law is explicit that "qualification as a foreign corporation under the laws of [the] Commonwealth" shall permit state courts to "exercise general personal jurisdiction" over a registered foreign corporation, just as they can over domestic entities. Pa. C.S.A. § 5301. Thus, by registering to do business in the Commonwealth of Pennsylvania and benefiting from the opportunity to do business in the Commonwealth of Pennsylvania, Optum has consented to being subject to general jurisdiction in the Commonwealth of Pennsylvania.

15. This Court also has specific personal jurisdiction over Defendants because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Additionally, the exercise of personal jurisdiction is proper because Defendants have

purposefully availed themselves of the privileges of conducting business within this District, and have established sufficient minimum contacts within the District.

16. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL BACKGROUND

A. Defendants Collected and Stored Plaintiff and Class Members' PII and PHI.

17. Change is a healthcare technology company that provides an array of medical business services, including revenue cycle management, healthcare analytics, and payment processing for patients, healthcare providers, and pharmacies (including processing of insurance claims).

18. Change is one of the largest healthcare technology companies in the United States and completes 15 billion healthcare transactions annually; as Change boasts on its website, one-third of *all* U.S. patient records are "touched by [its] clinical connectivity solutions."[9]

19. Change is integral to the functioning of the U.S. healthcare sector, acting as a digital intermediary that helps pharmacies verify patients' insurance coverage for prescriptions.

20. Since its acquisition by UnitedHealth in 2022, Change has operated as a "unit" of Optum. Optum's services are used to facilitate health care for 132 million individual consumers; nearly 130,000 physicians; 90% of U.S. hospitals; 67,000 U.S. pharmacies; and 80% of U.S. health plans across all fifty states and the District of Columbia.[10]

[9] Change Healthcare, *supra* note 3.
[10] *Investor Conference 2023: Overview & Highlights*, Optum, https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/ic23/UHG_IC23_Optum_Overview_Highlights.pdf (last visited Mar. 25, 2024).

21. UnitedHealth is ubiquitous in the United States healthcare system. Its umbrella of businesses touches nearly every aspect of the healthcare industry, including health insurance services, technology, data analytics, healthcare delivery, healthcare payor partner services, and more.[11] In 2023, UnitedHealth reported earnings of $371.6 billion,[12] ranking fifth on that year's Fortune 500 list.[13]

22. In the course of facilitating insurance and other transaction related to Plaintiff's and Class Members's healthcare, Defendants all receive, create, and handle patient PII and PHI, including, *inter alia*, names, addresses, Social Security numbers, medical records, payment information, prescription information, claims and insurance information, and other personal records.

23. Due to the sensitivity of the PII and PHI that Defendants handle, and their integral position in the healthcare system, Defendants are aware of their critical responsibility to safeguard their information systems as an outage of their network could jeopardize the health of millions of Americas, disrupting their access to vital mediations, and could subject individuals nationwide devastating consequences due to the theft of their sensitive personal information.

24. Despite the existence of these duties, Defendants failed to implement reasonable data security measures to safeguard their information systems, resulting in widescale disruption to the U.S. healthcare system, including patients' access to vital medication, and allowing nefarious third-party cybercriminals to compromise Plaintiff's and Class Members' PII and PHI.

---

[11] *Annual Report (Form 10-K)*, UnitedHealth Group (Feb. 28, 2024), https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/UNH-Q4-2023-Form-10-K.pdf.

[12] *UnitedHealth Group Q4 Earnings Report*, UnitedHealth Group (Jan. 12, 2024), https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/UNH-Q4-2023-Release.pdf.

[13] *Fortune 500*, Fortune, https://fortune.com/ranking/fortune500/ (last visited Mar. 25, 2024).

B. Defendants are Subject to Specific Duties under HIPAA as Business Associates of Healthcare Providers.

25. Upon information and belief, Defendants are "business associates" of healthcare providers (*i.e.*, "Covered Entities") who are governed by the privacy guidelines of the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.103.

26. As a regular and necessary part of their business, Defendants collect and maintain patients' highly sensitive PHI. As HIPAA Business Associates, Defendants are required under federal law to maintain the strictest confidentiality of any patients' PHI that it acquires, receives, and collects, and Defendants are further required to maintain sufficient safeguards to protect such PHI from being accessed by unauthorized third parties.

27. Indeed, whenever Defendants contract with Covered Entities to provide various business and medical services, HIPAA requires that these contracts mandate that Defendants will use adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing the HIPAA Security Rule[14] and immediately reporting any unauthorized use or disclosure of PHI (such as the Data Breach) to affected Covered Entities.

28. Change claims that it "is committed to the privacy and security of healthcare data and meets or exceeds HIPAA Privacy and Security Rule requirements."[15] Optum, too, claims to maintain protected information in compliance with HIPAA requirements.[16] Similarly,

[14] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[15] *HIPAA Simplified: Privacy and Security*, Change Healthcare, https://support.changehealthcare.com/customer-resources/hipaa-simplified/privacy-security (last visited Mar. 25, 2024).

[16] *Annual Report*, *supra* note 11. Notably, rather than discussing the impact that a breach would have on the 132 million patients it services, Optum solely mentions that non-compliance with

UnitedHealth acknowledges that it is "trusted and required to safeguard personal information reasonably and appropriately and to use or disclose such information only as authorized by the individual or in compliance with all applicable laws."[17]

29. Despite these assurances and Defendants' duty to safeguard Plaintiff's and Class Members' PII and PHI, Defendants employed inadequate data security measures to protect and secure the PII and PHI with which they were entrusted, resulting in the Data Breach.

C. The Risks of Storing Valuable PII and PHI Are Well-Known in the Healthcare Industry.

30. Given their roles in handling sensitive data, Defendants understood the PII and PHI they collect is highly sensitive and of significant value to those who would use it for wrongful purposes.

31. Defendants also knew that a breach of their computer systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

32. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Facebook, Target, Yahoo, and Marriott, as well as various healthcare partner and provider companies, including Anthem Blue Cross, LabCorp, Managed Care of North America, OneTouchPoint, Inc., Shields Healthcare Group, Eye Care Leaders and Connexin Software, Inc., and Blackbaud, Inc.

HIPAA would have an "adverse effect on our results of operations, financial position and cash flows." *Id.*

[17] *Code of Conduct*, UnitedHealth Group (2023), https://www.unitedhealthgroup.com/content/dam/UHG/PDF/About/UNH-Code-of-Conduct.pdf (last visited Mar. 25, 2024).

33. PII and PHI have considerable value and constitute enticing and well-known targets for cybercriminals. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[18] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

34. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States saw a 10% increase in the total number of data breaches in 2021 alone.[19]

35. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[20]

36. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[21] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have

---

[18] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[19] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[20] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Mar. 25, 2024).

[21] *The healthcare industry is at risk*, SwivelSecure, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Mar. 25, 2024).

reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[22]

37. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[23]

38. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[24]

39. In a 2022 report, the healthcare compliance company, Protenus, found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[25]

40. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of

[22] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names.
[23] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Mar. 25, 2024).
[24] *Id.*
[25] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Mar. 25, 2024).

healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[26]

41. Defendants' business, which touches nearly every aspect of healthcare, made them a particularly rich target for cybercriminals, in part, because of the extremely high value of the PII and PHI in their possession, including Social Security numbers, medical records, and health insurance information.

42. **Social Security Numbers—**healthcare data breaches often involve individuals' Social Security Numbers, which cannot be easily replaced—unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring an expansive review of the person's relationships with government agencies and private companies in order to update the person's accounts and profiles with those entities.

43. The Social Security Administration itself warns that the process of replacing an SSN is a difficult one that creates a separate set of problems, and cautions that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use

[26] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

> the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[27]

44. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security Numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security Numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

45. **Medical Records**—medical records in general are extremely lucrative for cybercriminals. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[28] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[29]

---

[27] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[28] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[29] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Mar. 25, 2024).

46. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[30]

47. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[31]

48. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.[32]

49. Identity theft victims often must spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which often includes paying off significant sums in fraudulent medical bills.

---

[30] Alder, *supra* note 22.
[31] *Id.*
[32] Brian O'Connor, *Health Care Data Breach: What to Know About Them and What to Do After One*, Experian (Mar. 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

50. **Health Insurance Information**—"stolen personal health insurance information can be used by criminals to obtain expensive medical services, devices and prescription medications, as well as to fraudulently acquire government benefits like Medicare or Medicaid."[33]

51. Victims of healthcare data breaches may be denied care, coverage, or reimbursement by their medical insurers, have their policies canceled, or have to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. At worst, victims of healthcare data breaches may even be threatened with losing custody of their children, be charged with drug trafficking, and face significant difficulty in keeping their jobs or finding employment.[34]

52. Stolen personal health insurance information also "can be used by criminals to obtain expensive medical services, devices and prescription medications, as well as to fraudulently acquire government benefits like Medicare or Medicaid."[35]

53. Once stolen, individuals' data will circulate on the Dark Web for years to come. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[36]

54. Even if stolen PII or PHI does not include specifically include financial, payment card, or medical account numbers and certain other information, the breach may still create a

---

[33] Kate O'Flaherty, *Why Cyber-Criminals Are Attacking Healthcare -- And How to Stop Them*, Forbes (Oct. 5, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/?sh=54e8ed1e7f69.
[34] *Id.*
[35] O'Flaherty, *supra* note 33.
[36] U.S. Gov't Accountability Off., Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Mar. 25, 2024).

substantial risk of identity theft. Using social engineering and "spear phishing" techniques, cybercriminals can use the limited information they have to lure victims into disclosing even more information. In these forms of attack, the criminal uses PII and PHI, such as a victim's name, address, email address, and known affiliation with a company or provider, to deceive the victim into providing additional data like their Social Security Number, medical history, or account numbers and passwords.

55. Based on the aforementioned cybercrime trends and the value of PII and PHI to cybercriminals, Defendants should have known the importance of safeguarding the PII and PHI with which they were entrusted, and of the foreseeable consequences if its data security systems were breached.

D. Defendants Knew the Risks Inherent to Maintaining Patients' PII and PHI.

56. Beyond these theoretical risks, Defendants had actual knowledge of the risk of collecting, maintaining, and safeguarding patients' PII and PHI.

57. As mentioned above, UnitedHealth acquired Change in 2022. However, prior to the acquisition, the Department of Justice ("DOJ") attempted to enjoin the purchase based on a variety of anticompetitive harms and risks to consumers—including the sheer amount of sensitive personal data over which UnitedHealth would have control through its subsidiaries post-acquisition.[37]

58. At the time, a DOJ representative publicly warned that the acquisition would "giv[e] UnitedHealth control of a critical data highway through which about half of all Americans' health insurance claims pass each year."[38]

---

[37] Complaint, *United States, et al. v. UnitedHealth Group Inc. et al.*, No. 1:22-cv-0481 (D.D.C. 2022).

[38] *Justice Department Sues to Block UnitedHealth Group's Acquisition of Change Healthcare*, Off. of Pub. Affs. Dep't of Just. (Feb. 24, 2022), https://www.justice.gov/opa/pr/justice-department-sues-block-unitedhealth-group-s-acquisition-change-healthcare.

59. Through these public statements, Defendants were put on notice about the risks associated with maintaining the vast amount of data processed through Change's systems.

60. Defendants have publicly acknowledged the risk of a cyber-attack as well. In UnitedHealth's most recent Annual Report, it noted the heightened risks of cyber-attacks and data security incidents, particularly those facing companies who were recently acquired:

> We routinely process, store and transmit large amounts of data in our operations, including protected personal information subject to privacy, security or data breach notification laws, as well as proprietary or confidential information relating to our business or third parties . . . We are regularly the target of attempted cyber-attacks and other security threats and have previously been, and may in the future be, subject to compromises of the information technology systems we use, information we hold, or information held on our behalf by third parties. . . .
>
> There have previously been and may be in the future heightened vulnerabilities due to the lack of physical supervision and on-site infrastructure for remote workforce operations and for recently-acquired or non-integrated businesses.[39]

61. A little over a year after UnitedHealth completed its purchase of Change, those vulnerabilities led to this Data Breach.

62. Defendants thus had actual and constructive knowledge of the value of PII and PHI to cybercriminals, the importance of safeguarding the PII and PHI with which they had been entrusted, and the foreseeable consequences of their systems were breached. Nonetheless, Defendants failed to take adequate cyber-security measures to prevent the Data Breach from occurring.

[39] *Annual Report*, *supra* note 11.

E. Defendants Breached their Duty to Protect Patient PII and PHI.

63. On February 21, 2024, UnitedHealth reported to the Securities and Exchange Commission ("SEC") that "a suspected nation-state associated cyber security threat actor" had gained access to Change's computer systems.[40]

64. Upon detection of this unauthorized access, UnitedHealth "immediately" isolated and disconnected the affected systems.[41] UnitedHealth also retained cybersecurity experts Mandiant and Palo Alto as part of its ongoing investigation.[42]

65. On February 28, 2024, a notorious ransomware gang known as ALPHV or Blackcat claimed responsibility for the cyberattack.[43]

66. Blackcat has attacked the computer systems of over 1,000 individuals and inflicted damage globally since its establishment, including networks essential to the functioning of critical U.S. infrastructure. In a December statement, the DOJ stated that Blackcat has become one of the most prolific ransomware-as-a-service variants in the world and has caused global losses in the hundreds of millions of dollars.[44]

---

[40] *Current Report (Form 8-K)*, UnitedHealth Group (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.
[41] *Id.*
[42] *Information on the Change Healthcare Cyber Response*, UnitedHealth Group, https://www.unitedhealthgroup.com/ns/changehealthcare.html (last visited Mar. 25, 2024).
[43] Sergiu Gatlan, *Ransomware Gang Claims They Stole 6TB of Change Healthcare Data*, BleepingComputer (Feb 28, 2024), https://www.bleepingcomputer.com/news/security/ransomware-gang-claims-they-stole-6tb-of-change-healthcare-data/.
[44] *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, Off. of Pub. Aff.'s, Dep't of Just. (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

67. Change confirmed on February 29, 2024, that the Data Breach was perpetrated by a cybercrime threat actor who represented itself as ALPHV/Blackcat.[45] That update has since been deleted.

68. Defendants have not confirmed what types of information were accessed and exfiltrated in the Data Breach.[46] However, per Blackcat's public claims, the cybercriminal group stole six terabytes of data belonging to "thousands of healthcare providers, insurance providers, pharmacies, etc.," allegedly including millions of people's medical records, insurance records, dental records, payments information, claims information, patient PII, and/or active U.S. military/navy personnel PII.[47]

69. The cyberattack and Data Breach has also caused widespread outages and disruptions to hospitals and pharmacies across the United States. For example, pharmacies across the country have reported that because of the Data Breach, they have unable to transmit electronic insurance claims for their patients, resulting in delays in getting prescriptions filled and thereby affecting patients' ability to access essential medications.[48]

70. Recognizing the severity of the Data Breach, the Department of Health and Human Services' Office for Civil Rights ("HHS") issued a "Dear Colleague" Letter, stating that the incident "poses a direct threat to critically needed patient care and essential operations of the health

[45] *Information on the Change Healthcare Cyber Response* (Archived), UnitedHealth Group, https://web.archive.org/web/20240301230118/https://www.unitedhealthgroup.com/ns/changehealthcare.html (archived from Mar. 1, 2024) (last visited Mar. 25, 2024).
[46] *Information on the Change Healthcare Cyber Response*, *supra* note 42.
[47] Gatlan, *supra* note 43.
[48] Christopher King, *Cyberattack on Change Healthcare paralyzes pharmacies across the US*, FOX5 Atlanta (Feb. 22, 2024), https://www.fox5atlanta.com/news/cyberattack-on-change-healthcare-paralyzes-pharmacies-across-the-us.

care industry." HHS further referred to the Data Breach as one of "unprecedent magnitude" and announced that it would be an initiating an investigation into the incident.[49]

71. To date, Defendants' investigation into the Data Breach is ongoing, and many of Change's systems are still down. A "Restoration Timeline" posted on UnitedHealth's website claims that certain "provider electronic payments [were] expected to be available for connection" on March 15, 2024 with phased reconnection of the claims system beginning March 18, 2024. As of the filing of this Complaint, Defendants are behind schedule on these posted restoration deadlines.[50]

F. Defendants Failed to Comply with FTC Guidelines and Industry Best Practices.

72. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

73. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[51]

---

[49] *HHS Office for Civil Rights Issues letter and Opens Investigation of Change Healthcare Cyberattack*, U.S. Dep't of Health & Human Servs. (Mar. 13, 2024), https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html.

[50] *Information on the Change Healthcare Cyber Response*, *supra* note 42.

[51] *Start with Security: A Guide for Business*, Fed. Trade Comm'n, August 2023, https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

74. In 2016, the FTC updated its publication titled Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.[52] The guidelines state that:

a. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;"

b. Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

e. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

75. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[53]

---

[52] *See Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n, October 2016, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[53] *Start with Security: A Guide for Business*, Fed. Trade Comm'n, August 2023, https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

76. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. Defendants were at all times fully aware of their obligations to protect the PII and PHI with which they were entrusted due to their position as business associate of covered entities, which gave it access to masses of patient PII and PHI. Defendants were also aware of the significant repercussions that would result from their failure to do so.

78. Upon information and belief, Defendants failed to properly implement one or more of the basic data security practices recommended by the FTC. Defendants' failure to employ reasonable and appropriate data security measures to protect against unauthorized access to patients' PII and/or PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

79. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[54]

80. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management

[54] *See Framework for Improving Critical Infrastructure Cybersecurity*, Nat'l Inst. of Standards and Tech. (April 16, 2018), Appendix A, Table 2, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[55] Defendants failed to adhere to the NIST guidance.

81. Further, cybersecurity experts have identified various best practices that should be implemented by healthcare industry entities, including the following measures:

a. Email protection systems and controls;

b. Endpoint protection systems;

c. Identify all users and audit access to data, application, systems, and endpoints;

d. Data protection and loss prevention measures;

e. IT asset management;

f. Network management;

g. Vulnerability management;

h. Security operations center & incident response; and

i. Cybersecurity oversight and governance policies, procedures, and processes.[56]

82. Upon information and belief, Defendants' failure to protect massive amounts of PII and PHI is a result of its failure to adopt reasonable safeguards as required by the FTC guidelines, NIST guidance, and industry best practices.

83. Defendants were well aware of their obligations to use reasonable measures to protect patients' PII and PHI. Defendants also knew they were a target for hackers, as discussed

[55] *Id.* at Table 2 pg. 26-43.
[56] *HICP's 10 Mitigating Practices*, HHS, https://405d.hhs.gov/best-practices (last visited Mar. 25, 2024).

above. Despite understanding the risks and consequences of inadequate data security, Defendants nevertheless failed to comply with its data security obligations.

G. Defendants are Obligated Under HIPAA to Safeguard Patient PHI.

84. As "business associates" of healthcare providers under HIPAA, Defendants are subject to minimum federal standards for privacy and security of PHI as set forth in under HIPAA and related regulations. *See* 45 C.F.R. § 160.103.

85. Defendants are required by HIPAA, 42 U.S.C. § 1320d *et seq*. to safeguard patient health information data and health information transactions.

86. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

87. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

88. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either "(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

89. HIPAA requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI;

(c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102 *et seq*.

90. The federal Department of Health and Human Services ("HHS") further recommends the following data security measures that regulated entities—such as Defendants—should implement to protect against cyber-attack techniques:

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[57]

91. Upon information and belief, Defendants failed to implement one or more of the recommended data security measures.

92. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals, nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

93. As such, Defendants are required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it acquires, receives, and collects, and Defendants are further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

94. Given the application of HIPAA to Defendants, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendants in order to receive healthcare services, Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

H. Plaintiff Has Experienced Significant Harm as a Result of the Data Breach.

95. Plaintiff is a patient whose prescriptions are electronically filled through Change's systems. In order to fill his prescriptions and get his necessary medications, Plaintiff was required to provide and entrust his providers, insurer, pharmacy, and Defendants with his PII and PHI. These

[57] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S. Dep't of Health & Human Services (Mar. 17, 2023), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

entities then provided Plaintiff's PII and PHI to Change to facilitate Plaintiff's prescription transactions.

96. In requesting and maintaining Plaintiff's PII and PHI, Defendants undertook a duty to act reasonably in its handling of Plaintiff's PII and PHI. Defendants, however, did not take care of Plaintiff's PII and PHI, leading to its exposure as a direct result of Defendants' inadequate data security measures.

97. Plaintiff was not notified of the Data Breach by Defendants. Unaware, Plaintiff visited his pharmacy in late February 2024 and attempted to fill one of his prescriptions with an electronic script. Plaintiff usually pays around $40 for this medication, but he was told by his pharmacy that he would have to pay $190 out-of-pocket due to the Data Breach. This unexpected, burdensome $150 price increase—the result of Change shutting down its systems in the aftermath of the Data Breach, and the resulting inability of his pharmacy to use his prescription savings card with his prescription—was how Plaintiff learned that his PII and PHI, and his providers' systems, were likely involved in the Data Breach.

98. Because Plaintiff could not fill his prescription though his pharmacy as a result of the Data Breach, Plaintiff was forced to spend his valuable time and effort going to another pharmacy to purchase the over-the-counter version of his medication with an out-of-pocket costs of approximately $38. This was approximately the same amount of money that he would normally spend on his prescription medication ($40), but the over-the-counter medication he purchased would only last him one week—as opposed to the one month's supply he typically receives when filling his prescription.

99. As a result of the Data Breach, Plaintiff incurred out-of-pocket expenses for medication he would normally have easy access to. This has caused Plaintiff to suffer stress and

anxiety about both having access to enough medication and the funds to pay for access to his medication so long has Change's systems remain down.

100. Since the Data Breach, Plaintiff has also been "bombarded" with spam call activity.

101. In addition, knowing that hackers likely accessed and exfiltrated his PII and PHI and will use that data for identity theft, fraud, and other nefarious purposes, which may create further disruptions in access to medication and healthcare, has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

102. Moreover, as a direct and proximate result of the Data Breach, Plaintiff has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending and is not speculative given the highly sensitive nature of the PII and PHI compromised in the Data Breach.

I. Plaintiff and Class Members Have Suffered Damages.

103. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members to suffer significant harm in several ways, including substantial and imminent risk of identity theft and fraud. Plaintiff and Class Members must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

104. Once PII and PHI are exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their

entire lives as a result of Defendants' conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

105. As a result of Defendants' failures, Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

106. With respect to healthcare breaches, another study found "the majority [70 percent] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[58]

107. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[59]

108. Indeed, PII and PHI are valuable commodities to identity thieves, and cybercriminals will trade stolen PII and PHI on the cyber black market for years thereafter. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security Numbers, and bank account information, complete with account routing numbers can fetch up to $1,200 to $1,300 each on the black market.[60] According to a report released by the FBI's cyber division, criminals can sell

[58] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HealthITSecurity, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited Mar. 25, 2024).
[59] *Id.*
[60] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC Media, (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited Mar. 25, 2024).

healthcare records for 50 times the price of stolen Social Security Numbers or credit card numbers.[61]

109. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[62]

110. PHI in particular is likely to be used in detrimental ways, by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[63]

111. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[64]

112. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect patient PII and PHI.

113. Plaintiff and Class Members have suffered emotional distress because of the Data Breach, the resulting increased risk of identity theft and financial fraud, and the unauthorized

---

[61] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited Mar. 25, 2024).

[62] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH, (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[63] *Id.*

[64] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Mar. 25, 2024).

exposure of their private medical information to strangers and their families, friends, and colleagues.

CLASS ACTION ALLEGATIONS

114. Plaintiff brings this class action on behalf of himself and all other similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure.

115. Plaintiff seeks to represent the following two Classes of persons defined as follows:

> **Medication Interruption Class**: All individuals in the United States who experienced disruptions to their prescription access as a result of the Data Breach of Change Healthcare systems reported on February 21, 2024.
>
> **Data Compromise Class**: All individuals in the United States whose PII and/or PHI was compromised in the Data Breach of Change Healthcare systems reported on February 21, 2024.

116. Excluded from each Class are Defendants, their subsidiaries and affiliates, officers and directors, any entities in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

117. This proposed class definitions are based on the information available to Plaintiff at this time. Plaintiff may modify each class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

118. **Numerosity:** The members of each Class are so numerous that the joinder of all members is impractical. Plaintiff is informed and believes, and thereon alleges, that there are millions of members of each Class described above, particularly given that Change handles 15 billion healthcare-related transactions annually. The exact size of each Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to

the files implicated in the Data Breach, but based on publicly available information the Data Compromise Class includes almost 79 million individuals.[65]

119. **Commonality:** This action involves questions of law and fact common to each Class. Such common questions include but are not limited to:

a. Whether Defendants had a duty to protect implement adequate data security measures to protect its computer systems from unauthorized access and related disruptions;

b. Whether Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;

c. Whether Defendants were negligent in collecting and storing Plaintiff and Class Members' PII and PHI, and breached their duties therein;

d. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

e. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

120. **Typicality:** Plaintiff's claims are typical of the claims of Members of each Class. Plaintiff's and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. For the Medication Interruption Class, Plaintiff and Class Members all had access to their prescription medications disrupted as result of Defendants' failure to

[65] Nick Hut, *Cyberattack on Change Healthcare brings turmoil to healthcare operations nationwide*, Healthcare Fin. Mgmt. Ass'n (March 20, 2024), https://www.hfma.org/technology/cybersecurity/cyberattack-on-change-healthcare-brings-turmoil-to-healthcare-operations-nationwide/.

implement adequate data security measures. For the Data Compromise Class, Plaintiff and Class Members each had their PII and PHI exposed and/or accessed by an unauthorized third party.

121. **Adequacy:** Plaintiff is an adequate representative of each Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class Members and has no interests antagonistic to the Class Members. Plaintiff also has no conflict that may arise from representing both Classes. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and all Class Members are substantially identical as explained above.

122. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

123. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

124. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

125. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff, the Medication Interruption Class, and the Data Compromise Class Against All Defendants)

126. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

127. Defendants owed a duty to Plaintiff and the Members of each Class to take reasonable care in managing and protecting the highly sensitive data they managed and stored on behalf of their clients. This duty arises from multiple sources.

128. Defendants owed a common law duty to Plaintiff and Members of each Class to implement reasonable data security measures because it was foreseeable that hackers would target Defendants' data systems, software, and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and Class Members would be harmed. Defendants alone controlled their technology, infrastructure, and cybersecurity. They further knew or should have known that if hackers breached their data systems, they would extract sensitive data and inflict injury upon Plaintiff and Data Compromise Class Members. Furthermore, Defendants knew or should have known that if hackers accessed Defendants' computer systems, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons (the Medication Interruption Class Members) who could no longer access prescription

medications while Defendants' computer systems were disrupted. Therefore, the Data Breach, and the harm it caused Plaintiff and Class Members, was the foreseeable consequence of Defendants' unsecure, unreasonable data security measures.

129. Additionally, Section 5 of the FTC Act, 15 U.S.C. § 45, required Defendants to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendants' duty to Plaintiff and Class Members. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants of failing to use reasonable measures to protect highly sensitive data. Defendants, therefore, were required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendants' duties to adequately protect sensitive information. By failing to implement reasonable data security measures, Defendants acted in violation of § 5 of the FTC Act.

130. Defendants are obligated to perform their business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendants to exercise reasonable care with respect to Plaintiff and Class Members by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and Class Members.

131. Defendants breached their duty to Plaintiff and Class Members by implementing unreasonable data security measures and by failing to keep data security "top-of-mind" despite demonstrating understanding of the risk of data breaches involving highly sensitive data and touting their own security capabilities.

132. Defendants were fully capable of preventing the Data Breach. Defendants, sophisticated and experienced technology companies, knew of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which would have prevented the Data Breach from occurring at all, or limited the scope and depth of the Data Breach. Defendants thus failed to take reasonable measures to secure their systems, creating vulnerability to a breach.

133. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Medication Interruption Class Members have suffered injuries, including, *inter alia*:

a. Costs associated with disruptions to their prescription medication access, such as out-of-pocket costs associated with acquiring alternative medications and not being able to fill their prescriptions at all; and

b. Emotional distress associated with the disruptions to their prescription medication access.

134. As a direct and proximate result of Defendants' negligence, Plaintiff and Data Compromise Class Members have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

135. As a direct and proximate result of Defendants' negligence, Plaintiff and all Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff, the Medication Interruption Class, and the Data Compromise Class Against All Defendants)

136. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

137. Pursuant to Section 5 of the FTC Act, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the PII and/or PHI of Plaintiff and Class Members.

138. Defendants breached their duties to Plaintiff and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII and/or PHI. Specifically, Defendants breached their duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

139. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants' duty.

140. It was reasonably foreseeable, particularly given the growing number of data breaches of PII and/or PHI within the healthcare industry, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and/or PHI in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiff and Class Members' unencrypted PII and/or PHI.

141. Plaintiff and Members of each Class are within the class of persons that the FTCA is intended to protect and Defendants' failure to comply with such constitutes negligence *per se*.

142. Furthermore, Defendants are covered entities as business associates under HIPAA, which sets minimum federal standards for privacy and security of PHI. a Pursuant to HIPAA, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations, Defendants had a duty to implement

and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

143. Specifically, HIPAA required Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102 *et seq.*

144. Defendants violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

145. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of Defendants' Customer Healthcare Providers.

146. Defendants' violation of HIPAA constitutes negligence *per se*.

147. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

148. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Medication Interruption Class Members have suffered injuries, including, *inter alia*:

a. Costs associated with disruptions to their prescription medication access, such as out-of-pocket costs associated with acquiring alternative medications and not being able to fill their prescriptions at all; and

b. Emotional distress associated with the disruptions to their prescription medication access.

149. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Data Compromise Class Members have suffered injuries, including, *inter alia*:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

150. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

151. In addition to monetary relief, Plaintiff and Data Compromise Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity theft monitoring to Plaintiff and Class Members.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Data Compromise Class Against All Defendants)

152. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

153. Plaintiff and Data Compromise Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

154. Plaintiff and Data Compromise Class Members conferred a monetary benefit upon

Defendants in the form of income that Defendants earn from transaction processing and related healthcare services that involve Plaintiff's and Class Members' PII and/or PHI. Defendants' business model would not exist save for the PII and/or PHI that is entrusted to them.

155. The relationship between individual consumers and Defendants is not attenuated, as Plaintiff and Data Compromise Class Members had a reasonable expectation that the security of their PII and PHI would be maintained when they provided their PII and PHI to Defendants' healthcare provider clients, including any third-party companies that these healthcare provider clients used to deliver healthcare.

156. Defendants accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Upon information and belief, this financial benefit was, in part, conferred, when Defendants were paid by clients to use Plaintiff's and Class Members' PII and PHI in the provision of their services. Defendants also benefitted from the receipt of Plaintiff's and Class Members' PII and PHI.

157. Defendants also understood and appreciated that the PII and PHI pertaining to Plaintiff and Data Compromise Class Members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of the PII and PHI.

158. But for Defendants' willingness to commit to properly and safely collecting and maintaining the security of Plaintiff's and Data Compromise Class Members' PII and PHI, their sensitive information would not have been transferred to and entrusted to Defendants. Further, if Defendants had disclosed that its data security measures were inadequate, Defendants would not have gained the trust of its healthcare provider clients and Plaintiff's and Data Compromise Compromise Class Members' data would not have ended up in Defendants' systems.

159. As a result of Defendants' wrongful conduct, Plaintiff and Data Compromise Class

Members suffered damages in an amount equal to the difference between what they paid for healthcare based on their expectations of reasonable data security and privacy practices, and the reduced value of those services due to a lack of reasonable data security and privacy practices and procedures.

160. Defendants' enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and use of Plaintiff's and Data Compromise Class Members' PII and PHI while at the same time failing to securely maintain that information from unauthorized access and compromise.

161. In particular, Defendants enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Data Compromise Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security.

162. Defendants should not be permitted to retain the money belonging to Plaintiff and Data Compromise Class Members. It would be unjust, inequitable, and unconscionable to retain the benefits it received and is still receiving from Plaintiff and Class Members because Defendants failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal and state laws and industry standards.

163. The benefit conferred upon, received, and enjoyed by Defendants was not conferred gratuitously, and it would be inequitable and unjust for Defendants to retain the benefit.

164. Plaintiff and Data Compromise Class Members are without an adequate remedy at law.

165. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Data Compromise Class Members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid, or Defendants should be compelled to place a percentage of all future profits into a common fund or constructive trust, for the benefit of Plaintiff and Data Compromise Class Members, designed to represent the value obtained by the use of the inadequately secured PII and/or PHI compromised as a result of the Data Breach.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff, the Medication Interruption Class, and the Data Compromise Class Against All Defendants)

166. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

167. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Class Action Complaint.

168. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and all Class Members' PII and PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI and/or cause an interruption in Defendants' services that prevent individuals from accessing medication. Plaintiff alleges that Defendants' data security measures

remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and PHI and remains at imminent risk that further compromises of his PII and/or PHI will occur in the future.

169. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. Defendants owed a legal duty to secure patient PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendants breached and continues to breach this legal duty by failing to employ reasonable measures to secure patient PII and PHI.

170. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' PII and PHI, and protect Defendants' systems from further breaches that disrupt their systems' functioning.

171. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of any of Defendants' systems. The risk of another such breach is real, immediate, and substantial. If another breach of any of Defendants' systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

172. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants

of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

173. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendants, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and patients whose confidential information would be further compromised.

DEMAND FOR JURY TRIAL

Please take notice that Plaintiff demands a trial by jury as to all issues so triable in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

A. For an order certifying each Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of each Class and Plaintiff's attorneys as Class Counsel to represent each Class;

B. For an order finding in favor of Plaintiff and each Class on all counts asserted herein;

C. For compensatory damages on behalf of Plaintiff and each Class;

D. For punitive damages on behalf of Plaintiff and each Class;

E. For an order of restitution and all other forms of equitable monetary relief;

F. Declaratory and injunctive relief as described herein;

G. For disgorgement and/or restitution as the Court deems appropriate, just, and proper;

H. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

I. Awarding pre- and post-judgment interest on any amounts awarded;

J. For reimbursement for all costs and expenses incurred in connection with the prosecution of these claims; and

K. Awarding of such other and further relief as may be just and proper.

Dated: March 25, 2024

Respectfully submitted,

/s/ Gary F. Lynch
Gary F. Lynch (PA ID No. 56887)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com

Counsel for Plaintiff and the Proposed Classes